

Exhibit C
Company Key Supplier Performance

As part of the ongoing efforts by Company to develop strong relationships with its key suppliers, suppliers will be evaluated on a periodic basis using Company's Key Supplier Management Process. The process will be administered either by a member of the Company's Procurement Team or through a named business stakeholder that may have a closer operational relationship with the supplier.

Included in the Key Supplier Management Process is the ongoing evaluation of the supplier performances based on the Agreement as well as other factors such as:

- Quality of products and/or services.
- Timeliness of delivery of goods and/or services.
- Responsiveness to problem resolutions.
- Cost comparison relative to competition and industry, including Total Cost of Ownership.
- Innovation and ability to add value.

As a "Key Supplier," Contractor agrees to provide monthly or quarterly Supplier Reports on products and/or services provided to Kmart/Sears. These reports will be developed in conjunction with a member of the Company Procurement Team and with a Contractor Representative. The reports are designed to provide additional supplier performance metrics as well as to provide an ongoing measure of requirements set forth in the Agreement to the Company Procurement Department. The Supplier Reports may include, but are not limited, to the following types of information:

- Quality of products and/or services.
- Quantity of products delivered and/or services performed, including YTD Totals.
- Prices charged to Kmart/Sears for products and/or services.
- Accuracy & timeliness of products and/or services delivered.
- Company's accrual of any qualified Rebates/Discounts based on the Agreement.

Company will provide the detailed questions that will be used for the supplier evaluation process. In addition, Company will provide Contractor with the requirements (content, format & frequency) of the Supplier Reports.

Contractor is encouraged to bring opportunities for improvement in the overall Procurement process to Company's attention.

Exhibit D

AFFILIATE ACCEPTANCE AGREEMENT

OF

[INSERT AFFILIATE'S NAME]

The undersigned Affiliate of **[insert Buyer name]** ("Affiliated Company") agrees to the terms set out in the Master Services Agreement dated **[insert date]** ("Agreement"), entered into between **[insert Buyer name]** and **[insert Contractor's name]** ("Contractor") as if Affiliated Company had entered into the Agreement. The terms and conditions of the Agreement are incorporated herein. Terms not defined in this acceptance form shall have the meanings specified in the Agreement.

Affiliated Company will place orders for the purchase of services directly to Contractor; Contractor will send invoices to the ordering Affiliated Company. Support for replacement parts, service plans, warranty administration, and equipment rentals will occur between the Affiliated Company and Contractor's participating authorized dealers serving such Affiliated Company. Contractor's dealers will send invoices to the ordering Affiliated Company for rentals, parts and/or services. Affiliated Company agrees to be financially responsible for all of its charges and obligations under the Agreement.

Affiliated Company's Legal Name Affiliated Company's Doing Business As Name Federal Tax ID Number

Street Address City State Zip Code

Primary Contact Primary Contact Telephone Number

Street Address City State Zip Code

By (Authorized Signature) Date

Printed Name of Person Signing Title

CONTRACTOR:

By: _____
(Authorized Signature) Date

Printed Name of Person Signing Title:

Exhibit E

Form for Addition or Removal of Location and/or Change to Services or Address

Exhibit A to the Master Services Agreement dated ____, 2014 by and between **Sears Holdings Management Corporation ("Sears")** and _____ (**hereafter referred to as "Contractor"**), (the "Agreement"), is hereby modified to change, add to, or remove from the current Exhibit B to the Agreement the following Location or Locations (the "Modification"):

(Complete the below as applicable):

1. The following Location is hereby added to Exhibit A:

Pricing for the new Location(s) listed above shall remain at the pricing terms set forth in the current Exhibit A.

2. The Service requirements or address of the following Location shall be changed as described below:

3. The following Location is hereby removed from the current Exhibit A:

In all other respects, the Agreement, as amended, remains in full force and effect in accordance with its terms.

Sears Holdings Management Corporation,

By: _____

Name:

Title:

Date: _____

Exhibit F

(Information Security)

At a minimum and as specified herein, Contractor shall provide security for all data and communication systems in support of the Agreement or Procurement Document to which this Exhibit F is attached (“**Exhibit**”).

Contractor’s security efforts will include, without limitation:

Logical Access Controls: Contractor agrees to employ effective logical access control measures over all systems used to create, transmit, or process SHMC Confidential Information), including but not limited to:

- User authentication must use unique identifiers (“**User ID’s**”) consistent with individual accountability; shared User ID’s do not provide the level of accountability required by SHMC;
- A complex password policy, including the prohibition of clear-text credentials must be enforced;
- User access rights/privileges to information resources containing SHMC Confidential Information must be granted on a need-to-know basis consistent with role-based authorization.
- User access to SHMC Confidential Information must be removed immediately upon user separation or role transfer eliminating valid business need for continued access.
- Default passwords and security parameters must be changed in third-party products/applications used to support SHMC Confidential.

Network Security Architecture: Contractor agrees to employ effective network security control measures over all systems used to create, transmit, or process SHMC Confidential Information including but not limited to:

- Firewalls shall be operational at all times and shall be installed at the network perimeter between Contractor’s internal (private) and public (Internet) networks.
- Properly configured and monitored IDS/IPS (Intrusion Detection/Prevention Systems) must be used on Contractor’s network.
- Databases must be logically or physically separated from the web server, and the database may not reside on the same host as the web server, where applicable.
- The database and other information systems used for the purposes of processing SHMC Confidential Information must have only those services/processes and ports enabled to perform routine business. All other services/processes on the host must be disabled.
- All information systems, repositories, etc. used for SHMC by Contractor, or its business partners, must be physically located in a controlled data center environment used for the purpose of protecting information systems.
- Secure channels (e.g., SSL, SFTP, SSH, IPSEC, etc.) must be used at all times for inter-host communications

Physical Access Controls: Contractor agrees to maintain servers, databases, and other hardware and/or software components that store information related to SHMC’s business activities in an access controlled and consistently monitored Data Center secured by appropriate alarm systems, which will not be

commingled with another unrelated party's hardware, software or information.

Risk Assessment: At no additional cost, Contractor agrees to provide responses to a risk assessment questionnaire (if provided by SHMC), participate in a passive scan of their network and / or application (upon notification).

- Contractor agrees to perform regular security vulnerability assessments and shall provide SHMC with results of a current security assessment by an accredited third-party (e.g., penetration test results of internet-facing devices, SAS 70-Type II reports, ISO 27001 certification, etc) as well as action plans describing how Contractor will address all identified security vulnerabilities affecting systems used to store, process or otherwise access SHMC Confidential Information.
- Contractor will permit SHMC or its designee to conduct audits of SHMC's data maintained or stored by the Contractor.

Security Policy: Contractor agrees to maintain and enforce security policies consistent with security best practices, and all applicable regulatory and legal security and privacy requirements, including but not limited to Massachusetts 201 CMR 17.00 et. seq. "Standards for the Protection of Personal Information of Residents of the Commonwealth". Upon request, Contractor shall provide copy of current security policy and standards as well as security architecture. Contractor shall comply with SHMC's Privacy Policy with respect to any SHMC customer personal information it receives.

Protection of SHMC Confidential Information: In addition to what may be described in the Agreement or Procurement Document to which this Exhibit is attached, Contractor agrees to protect SHMC Confidential Information as it would its own. For purposes of clarity, SHMC Confidential Information may include, but is not limited to, the following:

- Credit Card numbers
- Credit Card Validation Codes
- Personal Identification (PIN) numbers
- Loyalty Card Numbers with or without any associated PIN or Access Code
- Checking Account number (alone or in combination with checking account routing information)
- Bank Account number (alone or in combination with routing information)
- Drivers License Number or State-issued Identification Card Number
- Customer or Employee Names, in whole or in part
- Customer or Employee Postal Address
- Customer or Employee email address
- Date of Birth
- Social Security Numbers
- Health Insurance Card or Policy Identification Number
- Medical or Health Information
- Personal Telephone Number (when used with a customer/employee name or address)

Additionally, Contractor agrees to adhere to the following controls surrounding the use and protection of SHMC Confidential Information:

- Confidential information must be appropriately protected to the extent possible and/or encrypted (256-bit minimum) utilizing strong key management processes (e.g., access controls over keys, segregation of duties, documented processes, etc).
- Ensure secure processes and procedures (e.g., degaussing, anti-static bags, etc.) for handling or removal of physical media or equipment that may contain SHMC Confidential Information.
- Clear text (ftp, telnet, etc.) protocols may not be used to access or transfer SHMC Confidential information. SHMC Confidential Information must be encrypted when stored on portable media, which by way of example shall include USB Sticks, Portable hard drives, Laptops, DVD/CDs, and when transmitted on wireless networks or across public networks.
- SHMC Confidential Information may not be copied, sold or used for solicitation purposes by the Contractor or its business partners. SHMC Confidential Information may only be used in conjunction with and within the scope of the Procurement Document or the Agreement to which this Exhibit is attached.
- SHMC Confidential Information (data) must be segregated (physically and/or logically if in a database or virtual (VM) environment) from other Contractor customers. If data is not physically segregated from other customers, systems, or applications unrelated to SHMC, Contractor must provide appropriate data security controls over data at rest, including, access controls and encryption.
- Payment Card information must be masked on display rendering in a manner consistent with the Payment Card Industry Data Security Standard (PCI-DSS), the Fair and Accurate Credit Transaction Act (FACTA) and all other applicable laws and regulations.
- Contractor must disclose where SHMC data will be stored and processed. Storage and Processing of SHMC Confidential Information shall take place within the United States.
- **System Monitoring:** Contractor agrees to regularly audit and monitor information systems processing SHMC's business activities to ensure the protection of SHMC's information. Monitoring includes, but is not limited to, potential breaches or hacking activity and access to devices. Contractor must have defined processes for security alerting, escalation and remediation that are consistent with the Services procured pursuant to the Agreement. Contractor must ensure that event logs with SHMC data are not provided to other subscribers. If Contractor using virtual machines, must ensure there is granular monitoring of traffic that is crossing the virtual machine backplanes.

Vulnerability Management Controls: Contractor agrees to employ effective vulnerability management control measures over all of its systems used to create, transmit, or process SHMC Confidential Information, including; but, not limited to:

- Third-party vulnerability scans or audits of any external-facing (public) infrastructure devices.
- Annual third-party assessment of applications or processes supporting SHMC customer credit card information.
- Deploy and maintain currency of up-to-date commercially available anti-virus, anti-spam, anti-malware software on all information system components including personal computers, laptops, and interconnecting networks, where applicable, used for the purpose of managing SHMC Confidential Information. Additionally, provide for regular scanning for viral infections and update virus signature files frequently.

- Maintain a standard patch management process and practice to ensure the protection of any devices used to access, process or store SHMC Confidential Information. Contractor agrees to provide SHMC with their patch management policies and procedures upon request.
- Regularly auditing and monitoring to ensure the protection of SHMC Confidential Information.
- Any security breach that involves SHMC Confidential Information must be reported to SHMC in accordance with the Notice provision of the Agreement without unreasonable delay. Contractor shall immediately perform a root cause analysis as well as provide detailed information about measures taken by the Contractor to prevent future breaches. All efforts to rectify or resolve the situation must include subsequent and regular notification for the reported incident.
- Contractor agrees to provide full cooperation with SHMC and in the event of a data breach involving SHMC Confidential Information.
- SHMC must be immediately notified of any known attacks occurring against Contractor systems used to store or process SHMC Confidential Information.
- SHMC shall be immediately notified of security vulnerabilities that Contractor becomes aware of, and shall be subsequently be notified when said vulnerability is remediated, including a description of the specific remediation steps taken.

Data Recovery and Availability Contractor must provide detailed disaster recovery and business continuity plans that support the pre-defined recovery time objective (RTO) / recovery point objective (RPO) requirements defined by SHMC.

- Contractor must utilize industry best practices for data, services, and communications recoverability. Data and applications must be replicated across multiple independent sites and alternate communication channels must be available.
- Contractor is expected to validate and verify their existing capabilities through realistic scenario testing. Contractor must agree to participate in periodic recovery testing with SHMC. Proof of successful testing of the Contractor plan must be provided to SHMC upon request.
- Contractor systems must be device (computer machine) and provider independent in order to ensure portability and successful recovery of applications and backup or restoration services, or both.
- Contractor must provide company name, address, and contact information on all third-party relationships as well as services provided by each wherever those services create, transmit or process SHMC Confidential Information.

Data Destruction Contractor shall ensure that residual magnetic, optical, or electrical representation of SHMC Confidential Information that has been deleted may not be retrieved or reconstructed when storage media is transferred, become obsolete or is no longer usable or required by SHMC.

- Contractor should be utilizing minimum 256-bit encryption that renders data unreadable when storage is recycled, disposed of, or accessed by any means outside of authorized applications.
- Contractor data retention and destruction must align with SHMC requirements and policies as well as comply with applicable laws or regulations.
- SHMC information stored on Contractor media (e.g., hard drive, optical discs, tapes, paper, etc.) must be rendered unreadable or unattainable using the NIST Guidelines for Media Sanitization (Special Pub 800-88), prior to the media being recycled, disposed of, or moved off-site.



Certificate of Completion

Envelope Number: 068D771327E545308831BC28A45FA7C8

Status: Completed

Subject: Crown Equipment Corporation - CW2274461 - MSA

Source Envelope:

Document Pages: 83

Signatures: 2

Envelope Originator:

Certificate Pages: 2

Initials: 0

SHC Contract Management - P

AutoNav: Enabled

3333 Beverly Rd

Envelopeld Stamping: Enabled

Hoffman Estates, IL 60179

pitchaimani.marimuthu@searshc.com

IP Address: 119.226.198.138

Record Tracking

Status: Original

Holder: SHC Contract Management - P

Location: DocuSign

11/24/2014 1:37:55 PM CT

pitchaimani.marimuthu@searshc.com

Signer Events

Jim Smeltzly

jim.smeltzly@crown.com

Director, National Accounts

Security Level: Email, Account Authentication
(None)

Electronic Record and Signature Disclosure:
Not Offered
ID:

SHC Contract Management - P
pitchaimani.marimuthu@searshc.com

Contractor

Sears - Procurement

Security Level: Email, Account Authentication
(None)

Electronic Record and Signature Disclosure:
Not Offered
ID:

Hemant Porwal

Hemant.Porwal@searshc.com

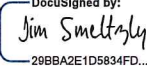
Vice President

Sears Holdings

Security Level: Email, Account Authentication
(None)

Electronic Record and Signature Disclosure:
Not Offered
ID:

Signature

DocuSigned by:

29BBA2E1D5834FD...

Using IP Address: 206.51.157.254

Completed

Using IP Address: 119.226.198.138

Timestamp

Sent: 11/24/2014 1:43:39 PM CT

Viewed: 12/1/2014 9:06:50 AM CT

Signed: 12/1/2014 10:46:59 AM CT

Sent: 12/1/2014 10:47:06 AM CT

Viewed: 12/9/2014 2:55:06 PM CT

Signed: 12/9/2014 2:55:14 PM CT

Sent: 12/9/2014 2:55:20 PM CT

Viewed: 12/9/2014 5:02:57 PM CT

Signed: 12/9/2014 5:03:22 PM CT

DocuSigned by:

9D719F0B9139402...

Using IP Address: 166.76.0.1

In Person Signer Events

Signature

Timestamp

Editor Delivery Events

Status

Timestamp

Agent Delivery Events

Status

Timestamp

Intermediary Delivery Events

Status

Timestamp

Certified Delivery Events

Status

Timestamp

Carbon Copy Events

Status

Timestamp

Carbon Copy Events	Status	Timestamp
<p>Andrea Cuervo Andrea.Cuervo@searshc.com Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Not Offered ID:</p>	COPIED	Sent: 12/1/2014 10:47:06 AM CT
<p>Andrea Cuervo Andrea.Cuervo@searshc.com Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Not Offered ID:</p>	COPIED	Sent: 12/9/2014 2:55:20 PM CT
<p>Andrea Cuervo Andrea.Cuervo@searshc.com Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Not Offered ID:</p>	COPIED	Sent: 12/9/2014 5:03:28 PM CT
<p>SHC Contract Management shccontractmgmt@searshc.com Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Not Offered ID:</p>	COPIED	Sent: 12/9/2014 5:03:28 PM CT

Notary Events	Timestamp
Envelope Summary Events	Timestamps
Envelope Sent	12/9/2014 5:03:28 PM CT
Certified Delivered	12/9/2014 5:03:28 PM CT
Signing Complete	12/9/2014 5:03:28 PM CT
Completed	12/9/2014 5:03:28 PM CT

